

Rozne ciekawe regulki iptables (wersja 0.6). Jakub Wartak <vnull@pcnet.com.pl>

Jesli masz cos ciekawego i chcesz sie podzielic - podeslij na maila.

1. Wykrywanie atakow DoS/virusow z naszej sieci i wycinanie ich wraz z przekierowaniem na WWW (idea by Lukasz Klimek z jakiegos PDF – SZLUG?, realizacja – ja ;)):

```
# zmienic!
PORT_FAKEDNS=1053
PORT_WWW_VIRUS=81
SERVER_FAKEDNS=195.117.92.20
SERVER_WWW=195.117.92.23

modprobe ip_set

ipset --create badports portmap --from 1 --to 65000
ipset --create ours nethash

ipset -A ours 10.0.0.0/8
ipset -A ours 195.117.92.0/24
ipset -A ours 80.51.8.0/24
...

# set z zlymi portami ( zainfekowane maszyny sie do tych portow lacza )
ipset -A badports 135
ipset -A badports 1111
...

# przywiazanie badports do ours
ipset -B ours :default: -b badports

# target ktory bedzie przekierowywal ruch WWW i DNSy a reszte wycinal
iptables -t nat -N dnat_virus
iptables -t nat -A dnat_virus -p udp --dport 53 -j DNAT --to-destination $SERVER_FAKEDNS:$PORT_FAKEDNS
iptables -t nat -A dnat_virus -p tcp --dport 80 -j DNAT --to-destination $SERVER_WWW:$PORT_WWW_VIRUS
iptables -t nat -A dnat_virus -j DROP

# jesli jest taki Ipek na liscie to wymusza okres ciszy dla niego,
# kazdy kolejny pakiet przedluzy zawsze o 1h wyciecie+przekierowanie
iptables -t nat -A PREROUTING -m recent --name antidos --update --seconds 3600 -j dnat_virus

iptables -t nat -N MYIPLIMIT
# czy slemy do 2 polaczen/s ? --> jesli tak , to wychodzimy stad
iptables -t nat -A MYIPLIMIT -m hashlimit --hashlimit 2/sec --hashlimit-mode srcip --hashlimit-name MYIPLIMIT -j RETURN
# slemy ponad 2 polaczenia/s --> dodajemy do recent Ipeka ktory to robi,
# aktualne polaczenie dropujemy
iptables -t nat -A MYIPLIMIT -m recent --name antidos --set -j DROP
```

```
# 0. tcp?
# 1. czy jest to nowe polaczenie?
# 2. czy jest z naszej klasy ?
# 3. czy jest to pakiet do zlego portu?
# 4. jesli dotad wszystko sie zgadza to idziemy do MYIPLIMIT
```

```
iptables -t nat -A PREROUTING
    -p tcp \
    -m state --state NEW \
    -m set --set ours src,dst \
    -j MYIPLIMIT
```

```
# UWAGA1: na $PORT_FAKEDNS znajduje sie prymitywny serwerek DNS filtrujacy napisany w Perlu,
#          odpowiadajacy "127.0.0.1" na wiekszosc zapytan ;) -- moze kiedys udostepnie
```

2. Ze strony Lemata (<http://lemat.priv.pl>):

```
iptables -A FORWARD -m state --state RELATED, ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -m recent --name FTP --seconds 60 --update -j DROP
iptables -A FORWARD -p tcp --dport 21 -m limit --limit 5/second --limit-burst 15 -m recent --name FTP --set -j
ACCEPT
```

3. Ladna prioretyzacja:

```
# albo nawet nethash i dawac cale maski
```

```
ipset --create gry iphash
ipset -A gry serw1
ipset -A gry serw2
```

```
...
```

```
ipset --create gryporty portmap --from 1 --to 65535
```

```
ipset -A gryporty port1
```

```
...
```

```
# bind
```

```
ipset -B gry :default: -b gryporty
```

```
# klasyfikuje na wyjsciu do neta do serwerow i portow docelowych
```

```
#jednoczensie,
```

```
iptables -t mangle -A POSTROUTING -o $WAN_IF -p tcp -m set --set gry dst,dst -j CLASSIFY blahgry
```

```
iptables -t mangle -A POSTROUTING -o $WAN_IF -p udp -m set --set gry dst,dst -j CLASSIFY blahgry
```

```
# klasyfikuje na wyjsciu do lanu od serwerow i od portow jednocznesie
```

```
iptables -t mangle -A POSTROUTING -o $LAN_IF -p tcp -m set --set gry src,src -j CLASSIFY blahgry
```

```
iptables -t mangle -A POSTROUTING -o $LAN_IF -p udp -m set --set gry src,src -j CLASSIFY blahgry
```

```
# blahgry to rzecz jasna kolejka utworzona na ifach dla gier specjalnie...
```

4. Przykład ochrony usługi przed DDoS na serwerze/firewallu:

```
iptables -t raw -N ANTIDOS
iptables -t raw -A ANTIDOS -m hashlimit --hashlimit 5/s \
    --hashlimit-name limitDoS --hashlimit-mode srcip,dstport -j ACCEPT
iptables -t raw -A ANTIDOS -j DROP
iptables -t raw -A PREROUTING -i eth0 -p tcp --syn -j ANTIDOS
```

5. Ograniczanie ilości pps-ów per IP w sieci:

```
iptables -t raw -N limitPPS
# jeśli ślemy mniej niż limit to wychodzimy
iptables -t raw -A limitPPS -m hashlimit --hashlimit 80/s --hashlimit-name limitPPS \
    --hashlimit-mode srcip -j RETURN
# więcej niż 80/s => DROP
iptables -t raw -A limitPPS -j DROP

# niemy od klientów
iptables -t raw -A PREROUTING -i $LAN_IF -j limitPPS

# niemy do klientów
iptables -t raw -A PREROUTING -o $LAN_IF -j limitPPS

# UWAGA1: statystyki można sprawdzać w /proc/net/ipt_hashlimit/limitPPS
# UWAGA2: 256 kbps można wysycić w ~21 pakietach/s (przy rozmiarze pakietu 1500 bajtów)
```

6. Ograniczanie ilości równoległych połączeń TCP (klienci => net):

```
iptables -A FORWARD -i $LAN_IF -p tcp --syn -m connlimit --connlimit-above 100 --connlimit-mask 32 \
    -j REJECT --reject-with tcp-reset

# UWAGA1: łatwo z tego zrobić ograniczenie tylko dla P2P łapanego przez ipp2p czy l7-filter
# UWAGA2: można zamiast "--syn" dać też "--m state --state ESTABLISHED"
```

7. Inne pomysły (zrealizowane bądź w testach, ale tymczasowo tutaj nie będą publikowane):

- a) wylapywanie ruchu złego, wsadzanie IPeKa do iptree (-j SET), klasyfikowanie całego ruchu z/do tego zbanowanego IPeKa jako najmniej uprzywiejowanego (oparte na HFSC)
- b) CLASSIFY + PRIO + HFSC (bardzo ładnie się sprawdza dla VOIPa i ICMP-ping/gry)

8. cos tu jeszcze będzie :)